Secure and Fast PIN-entry Method for 3D Display

Mun-Kyu Lee, Hyeonjin Nam
School of Computer and Information Engineering
Inha University
Incheon, Korea
e-mail: mklee@inha.ac.kr, jin0639@hanmail.net

Abstract—**The personal identification number (PIN) is one of the most well-known user authentication methods. However, there have been concerns about the security of the regular PIN pad against shoulder surfing attacks. Although there are many indirect input methods based on random challenges, most of them have usability issues because they require very long authentication time and their error rates are quite high. In this paper, we introduce our ongoing work to develop a solution to this problem using a 3D display. The proposed method transmits a random challenge to a user more effectively and securely by displaying a specific challenge object with different 3D depth from the other decoy objects. A prototype of the proposed method was implemented on a smartphone with a parallax barrier-based glasses-free 3D LCD, which guarantees the physical security because only a legitimate user who is located at the right position in front of the device can recognize the 3D effect correctly, while an attacker cannot. According to our pilot test, the average authentication time and the average error rate of the proposed method are as small as 8.4 seconds and 5.0%, respectively.**

Keywords-personal identification number, authentication, smart device, 3D display

I. INTRODUCTION

User authentication is a procedure that verifies the identity and access permission of a claimed user. It is well known that there are three categories for user authentication; knowledge-based authentication, hardware token-based authentication, and biometric verification. In this paper, we are interested in the first category, which is the most prevalent one. Especially, we will focus on personal identification number (PIN).

Although PINs are widely used for smart devices, ATMs, and digital door locks, there are concerns about the security of PINs [1]. That is, anyone who observes the authentication procedure over the user's shoulder can easily impersonate the user, because the traditional PIN pad asks a user to directly input his/her PIN and this PIN is short enough for an ordinary human attacker can memorize to use in the next authentication session. This kind of attack is known as a shoulder surfing attack [2].

We can find many proposals to solve this issue in the security literature [2-6]. They were designed so that a user may enter a response to a random challenge given by the system instead of entering the PIN digits directly. The response is computed by combining properly the challenge and the secret PIN. However, the previous methods have usability issues. That is, they require too long time to enter a PIN or their error rates are too high. The major reason for this is that the procedure where the user computes an appropriate response from the given challenge is very complex due to security requirement.

In this work, we propose a solution to this problem, which is applicable to devices with a 3D display. The proposed method effectively transmits a challenge to a user by showing a challenge object with distinct 3D aspects from the other decoy elements. The challenge object defines a simple mapping between PIN digits and some alphabet characters. Then, the user only has to remember this mapping, and inputs the mapped characters though a keypad. On the other hand, the attackers without access to the 3D information cannot obtain any information about the challenge object. According to the pilot test, the PIN-entry time and error rate of the proposed method are significantly smaller than those of the existing methods. We name our method Map-3D after the design principle.

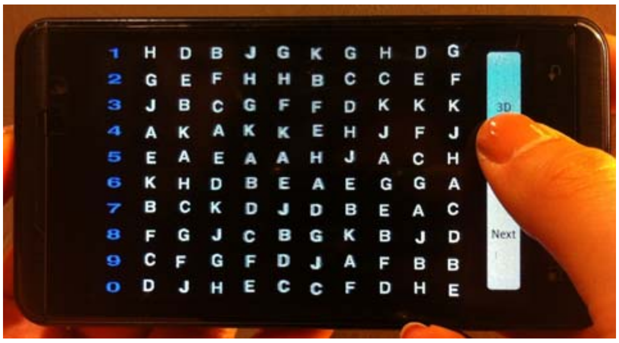
The remainder of this paper is organized as follows. Section 2 gives a brief introduction to the 3D display technology that we used to implement our proposal. The proposed method is explained in Section 3. Section 4 and Section 5 analyze the security and practical performance of the proposed method, respectively. Section 6 compares the proposed method with previously known methods. Section 7 enumerates the issues that we still have to resolve and propose future work.

II. 3D DISPLAY

Nowadays, we see many devices with 3D display, such as a 3D TV, a 3D monitor, a 3D game console, a 3D smartphone, and a 3D smart pad. Although the proposed method may be applicable to any of these devices, we consider a 3D smartphone as the implementation platform for this paper. We used an LG Optimus 3D smartphone with a parallax barrier 3D LCD whose resolution is 800 by 480 pixels. The parallax barrier [7] is a well-known method to realize glasses-free 3D display, where many thin vertical slits are regularly placed in front of an LCD so that the left and right eyes may see different sets of pixels. The difference between the images for left and right eyes produces a stereoscopic effect. However, this effect is only realized at a specific point in front of the screen, where the eyes of the legitimate user should be located. If the eyes are not at this position, the user will not recognize the 3D effect correctly. Naturally, the attacker will not be able to feel the 3D effect because s/he cannot be at this sweet spot. In this way, the security of our method is physically guaranteed.

III. MAP-3D: PROPOSED METHOD

Figure 1 shows the layout of Map-3D, the new method. Map-3D is composed of two stages; the challenge display stage and the response input stage. Figure 1 is the first stage, where a 10 by 10 matrix of alphabets is given to the user as well as the row index from 1 to 0 and two touch buttons labeled '3D' and 'Next.' Each column is a random permutation of 10 alphabet characters from A through K. (We do not use letter I because it may be confused with integer 1.) As a result, each character appears exactly 10 times in the matrix. Initially, all 100 letters are displayed with the same 3D depth. When the user touches the '3D' button, the device changes the depths of letters. To be precise, a random one among 100 letters is chosen by the device, and it is displayed with depth +1, and all the other letters with depth -1, where positive and negative depths mean that an object is displayed as a prominent and depressed letter, respectively. In the example of Fig.1, the 'F' at the intersection of row 9 and column 2 is at depth +1, and it is shown to the user as a prominent letter. (Unfortunately, we cannot express the 3D effect properly on this printed paper. In fact, the picture in Fig. 1 that was taken using an ordinary 2D camera is roughly what the attacker sees.) The other 99 letters are displayed on the plane with depth -1, and the user will feel as if these letters are depressed. While the user keeps touching the '3D' button, this 3D effect is maintained.



1	H	D	B	J	G	K	G	H	D	G
2	G	E	F	H	H	B	C	C	E	F
3	J	B	C	G	F	F	D	K	K	K
4	A	K	A	K	K	E	H	J	F	J
5	E	A	E	A	A	H	J	A	C	H
6	K	H	D	B	E	A	E	G	G	A
7	B	C	K	D	J	D	B	E	A	C
8	F	G	J	C	B	G	K	B	J	D
9	C	F	G	F	D	J	A	F	B	B
0	D	J	H	E	C	C	F	D	H	E

Figure 1. Challenge display stage of Map-3D.

After recognizing the prominent letter F, the user releases the button, which eliminates the 3D effect. But, the arrangement of letters remains the same. Then, the user's task is to remember 4 specific letters in his/her short-term memory. For example, let's assume that the PIN is '6421.' The user focuses on the second column where the prominent F was located, and remembers the 4 letters at rows 6, 4, 2, and 1, which are H, K, E, and D, respectively. In the case that the user forgets the prominent letter, s/he may touch again the '3D' button to reshow the 3D effect. But, at this time, the device chooses again a new random letter to be displayed with depth +1. The user finishes the challenge display stage by touching the 'Next' button. This immediately starts the response input stage.

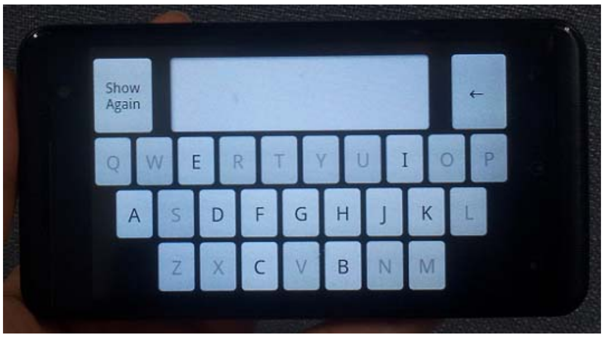


Figure 2. Response input stage of Map-3D using QWERTY keypad.

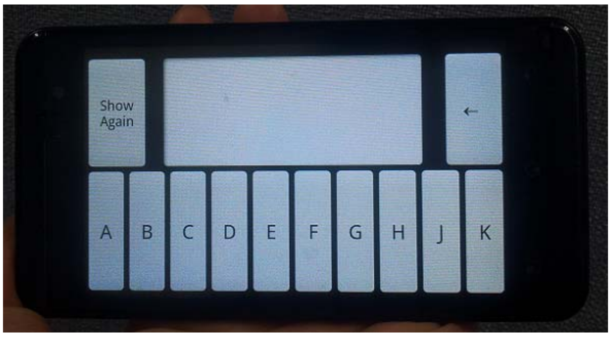


Figure 3. Response input stage of Map-3D using linear keypad.

In the response input stage, the device displays an ordinary keypad as in Fig. 2. However, the input of letters that do not belong to the challenge alphabet set is disabled. The user only has to input the four letters that s/he memorized in the first stage. An alternative input method shown in Fig. 3 is also possible. In this case, the 10 possible letters are displayed in a row.

IV. SECURITY

For security analysis, we may consider two criteria, because an attacker may have two different attack strategies; random guessing and shoulder surfing [8]. With the random guessing strategy, the attacker tries to pass the authentication test by randomly selecting the possible responses. We easily see that the success probability of this strategy is 1/10,000, which is the same as that of a regular PIN pad.

On the other hand, in a shoulder surfing attack scenario, the attacker tries to obtain useful information on the PIN by observing the authentication session of a legitimate user. Because the depths of all letters in the challenge display stage will look the same to the attacker who is not at a right position, the only thing the attacker can do is to carefully remember the arrangements of 100 letters and the 4 letters that the user enters in the response input stage. However, it is well known that a human user can remember only 7±2 items in the short-term memory [9], and recent research results show that the number of items is actually even less than this value [10]. However, at this point, let's assume very pessimistically, that an attacker may memorize 10 items at the same time. Then, the best strategy will be to randomly choose one column and to memorize the 10 elements in that column. Combining this information and the user's response, the attacker can recover the PIN digits with a probability, 1/10. This is 10 times less than that of the regular PIN pad. Therefore, we conclude that the proposed method is significantly safer than the regular PIN pad against a shoulder surfing attack. However, we remark that even this estimation is a very pessimistic one, and we conjecture that the real probability will be far less than 1/10.

V. Implementation and Performance Analysis

For our pilot test, we used LG Optimus 3D smartphone. The software for the proposed method was programmed using Java over Android 2.3.3. We start this section by explaining the implementation details for 3D effects. As explained in the Section 3, a prominent object is given a positive depth, while a negative depth implies that an object is located at a deeper plane. This difference in depth is realized by showing different images to left and right eyes. If the depth is 0, two eyes see the same images. However, for positive and negative depths, the object is horizontally shifted by proper amount. For example, if the depth of an object is +1, the object should go to right by one position in the image for the left eye. Similarly, it should go left by the same amount in the image for the right eye.

We designed a pilot test to verify the validity of our idea. We recruited four subjects from our local university. Their ages were between 21 and 40. Two of them were male. Before the test, we explained the rationale for our proposal and the authentication procedure. The participants easily understood the working principle of the proposed method, and we did not give them any opportunity for practice. But we measured the timing and error rate from their first trials. Each participant performed ten authentication sessions with the QWERTY keypad shown in Fig. 2. Then, ten additional sessions were performed with the linear keypad in Fig. 3.

According to the experimental results, the average authentication time among the 40 sessions with the QWERTY keypad was 8.4 seconds, and the best one was as fast as 5.2 seconds. There was no significant difference in the case with the linear keypad. The average was 8.5 seconds, and the minimum was 5.4 seconds. The error rates in two experiments were 5.0% and 7.5%, respectively, where an error is defined as the case that the user completes the session but the entered PIN is different from the correct one. We remark that there were only 10 among 80 sessions where a participant touched the '3D' button more than once.

VI. Comparison with Related Works

In Table 1, we compare the performance of the proposed method with those of the previous methods including the legacy PIN pad. Table 1 lists the authentication times and error rates of various methods including the proposed one. We remark that the data for the previous methods are not from our own experiments, but they are from the papers that presented each method. But we recalculated error rates of some methods because their definition of error rate is different from ours. That is, they defined an error as the case that the user enters incorrect PINs in three consecutive trials, which is a common practice in ATMs. If we adopt this definition, the error rate of the proposed method is 0. However, we define an error as the case that the user enters an incorrect PIN in one trial.

TABLE I. Comparison of Speed and Error Rate

Method	Authentication time	Error rate
Regular PIN pad	< 3	≈ 0
Binary [2]	23.2	9.0
Undercover [3]	32-45	> 31.5
VibraPass [4]	8.2	> 14.8
Haptic Wheel [5] [a]	23.0	16.4
ColorPIN [6] [a]	13.3-13.9	N.A.
Proposed: Qwerty	8.4	5.0
Proposed: linear keypad	8.5	7.5

a. Audio-based version

According to Table 1, the speed of the proposed method is much faster than those of the existing methods, except the regular PIN pad, which does not have shoulder-surfing resistance and VibraPass whose error rate is too high. The error rate of the proposed method is also very low compared to the other challenge-response-based methods.

VII. Future Work

This paper is a description of work in progress that still has several factors to be addressed as follows:

- In the first stage of the current version, the digits from 1 to 0 are arranged vertically. The horizontal arrangement could be considered. In addition, the number of letters assigned to a digit should not be always 10, but it may be customized.
- The depth difference between the prominent letter and the remaining letters are 2 in the current version. We may try other values for better 3D effect.
- In the first stage, only the letters from A to K are given to the user. We may consider a complete set of capical letters, i.e., A to Z. In this case, the impact on the security and performance should be analyzed.
- The pilot test in this paper only involves 4 subjects. We need to perform a complete test with more participants with diverse demographic backgrounds. Especially, applicability to the subjects with vision problems would be an interesting issue.
- It would be meaningful to verify if there is any significant learning effect. Therefore, we may analyze the transition of authentication times and error rates according to the accumulated number of trials through a long-term study.
- We may also redesign the experiment so that the device may present instructions that participants should follow. In the current experiments, we directly explained the new system to the participants.
- We may also try to apply the new method to non-hand-held devices such as an ATM. There are several devices available on the market to simulate this situation, e.g., 3D smart pads, although most of them require 3D glasses.

In our future work, we will continue our research to present a complete version of the proposed method as well as more extensive analysis results.

ACKNOWLEDGMENT

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center)) support program (NIPA-2013-H0301-13-1003) supervised by the NIPA (National IT Industry Promotion Agency) and the IT R&D program of MOTIE/KEIT. [10039180, Intuitive, convenient, and secure HCI-based usable security technologies for mobile authentication and security enhancement in mobile computing environments].

REFERENCES

[1] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? The security of customerchosen banking PINs," Financial Cryptography and Data Security 2012, Feb. 2012, pp. 25-40.

[2] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," Proceedings of the 11th ACM Conference on Computer and Communications Security, Oct. 2004, pp. 236-245.

[3] H. Sasamoto, N. Christin, and E. Hayshi, "Undercover: Authentication Usable in Front of Prying Eyes," CHI 2008, April 2008, pp. 183-192.

[4] A. D. Luca, E. V. Zezschwitz, and H. Hußmann, "VibraPass-Secure Authentication Based on Shared Lies," CHI 2009, April 2009, pp. 913-916.

[5] A. Bianchi, I. Oakley, J. K. Lee, and D. S. Kwon, "The Haptic Wheel: Design & Evaluation of a Tactile Password System," CHI 2010, April 2010, pp. 3625-3630.

[6] A. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN – securing PIN entry through indirect input," CHI 2010, April 2010, pp.1103-1106.

[7] Parallax barrier, http://en.wikipedia.org/wiki/Parallax_barrier. [retrieved: May, 2013]

[8] Q. Yang, J. Han, Y. Li, and R. Deng, "On limitations of designing leakage-resilient password systems: attacks, principles and usability," The 19th Annual Network & Distributed System Security Symposium (NDSS 2012), Feb. 2012.

[9] G. A. Miller, "The magical number seven, plus or minus two: some limits on our capacity for processing information," Psychological Review, vol. 63, 1956, pp. 81–97.

[10] G. A. Alvarez and P. Cavanagh, "The capacity of visual short-term memory is set both by visual information load and by number of objects," Psychological Science, vol. 15, no. 2, 2004, pp. 106–111.